ABSTRACT OF THE DISCLOSURE

Presented is a method and system for improving the efficiency of network security protections communication protocols such as Secure Socket Layer ("SSL") using enhanced Rivest-Shamir-Adleman ("RSA") encryption and decryption techniques. During the establishment of the initial handshake of SSL communications, where a client is coupled to a server, the server generates a RSA public / private key pair. The public key is formed using two distinct prime numbers. By reducing the size of these prime numbers and arriving at the decrypted message using the Chinese Remainder Theorem, the efficiency of establishing a secure communications session is increased. Likewise if during generation of the public key, the prime numbers possess a mathematical relationship to the public key such that the prime numbers are on the order of a third of the size of the public key then the efficiency of establishing the initial handshake is again improved.